2014

Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours

Koteswara Ivaturi
University of Auckland, k.ivaturi@auckland.ac.nz

Lech Janczewski
University of Auckland, lech@auckland.ac.nz

Cecil Chua
University of Auckland, aeh.chua@auckland.ac.nz

8R. Effect of Frame of Mind on Users' Deception Detection Attitudes and Behaviours

Koteswara Ivaturi
University of Auckland
k.ivaturi@auckland.ac.nz

Lech Janczewski
University of Auckland
lech@auckland.ac.nz

Cecil Chua
University of Auckland
aeh.chua@auckland.ac.nz

Abstract

As the World Wide Web grows, the number and variety of deceptive attacks targeting online consumers likewise increases. Extant research has examined online deception from an information processing perspective, that is, how users process information when they encounter deceptive attacks. However, users' ability to process information is based on what the users are thinking or their frame of mind while engaged with that information. Frame of mind has not been well studied in the security domain. This study proposes the effect of users' frame of mind on their attitude towards online deception and their actual deception detection behaviour. Specifically, we propose that human information needs and the framing (positive or negative) of important information such as warnings are significant components of users' frames of mind that impact their vulnerability to online attacks. We conclude the paper by discussing in detail the experimental setup and expected contributions from the analysis.

Keywords

Online deception, frame of mind, information seeking, information processing

1. Introduction

Cybercrime is a growing and unsolved phenomenon which continues to cause significant costs to both individuals and organizations. It is estimated that 65% of people using the Internet have been subjected to some form of cybercrime (Norton, 2010). The annual turnover of the global cybercrime industry is estimated at US$ 1 trillion (Kshetri, 2010; Menn, 2010). Most modern cybercrime does not rely wholly on technological mechanisms to overcome security systems. Instead, it relies mostly on human behaviour (Townsend, 2010). Thus, modern computer security relies on users to make the correct decisions when faced with a cyber-attack. Unfortunately, extant research tells us that users often make poor decisions when faced with cyber-attacks (Ekman, 2009).

Most research that examines users' ability to detect online deception leverages on the mechanics of human information processing (Biros, George, & Zmud, 2002; Burgoon & Buller, 1996; Johnson, Grazioli, Jamal, & Glen Berryman, 2001). One underexplored, but likely predictor of human information processing (and therefore a user's ability to detect online deception), is a user's frame of mind. This, in turn, can be affected by the activity the user is performing. As an analogy, consider how a user's frame of mind influences driving safety. Substantial research has shown that other activities the user is performing while driving such as making or receiving a mobile phone call or using a hands-free device impacts driving safety performance (Redelmeier & Tibshirani, 1997). Accordingly, the distracted

frame of mind compromises driving safety. In the same way, we argue the user's vulnerability to online attacks depends directly on the user's frame of mind while performing tasks.

Online users engage with different kinds of web applications to cater to their multitude of information needs. Accordingly, users' specific frame of mind has an effect on the kind of information that users are in need of and the methodology employed to seek for it. For example, if a person is looking for a very specific piece of information, the person will probably use a search engine. In contrast, if this person is not looking for anything specific, but is willing to serendipitously discover information, the person might just spend time browsing a newsgroup or forum. Finally, users of email and social networks are not looking for anything specific but are constantly monitoring their accounts to find useful information. Another factor that affects the user's frame of mind is whether the user views an information source as suspicious or not (e.g., the user has been warned).

Leveraging on research on human information behaviour, we argue that the particular activity users perform influences their frame of mind, thereby making them more or less vulnerable to attacks. Our paper proposes contribution to research in three ways. First, our paper proposes that users engaged in active seeking (e.g., searching the web) are more vulnerable to cyber-attacks than users engaged in non-directed monitoring (e.g., browsing forums), who are in turn more vulnerable than those engaged in active scanning (e.g., reading email). Furthermore, we also propose that users who are warned are less vulnerable than users who are not.

The paper is organized as follows. In the next section, we give a brief overview of the background literature on online deception. We then build our argument towards the frame of mind concept, leveraging on the information seeking and security awareness literature. In the following section we present our research model and supporting arguments for the hypotheses. Next, we discuss the experiment and the procedures involved along with information about the sample. We then discuss the analysis method that will be used for the study and conclude with expected contributions.

2. Background & Prior Literature

It is widely accepted that humans are the weakest links in any security infrastructure (Mitnick & Simon, 2003). This has prompted many IS security researchers to study the phenomenon of human behaviour and decision-making ability in the light of security attacks. The majority of such studies find that humans, even experienced ones, are poor detectors of deception (Ekman, 2009; Stefano Grazioli, 2004; S. Grazioli & Jarvenpaa, 2000). Most of such studies have adopted a view that when users encounter any information-laden stimulus, they process or interpret information in the stimulus to make decisions about the credibility of the information. For example, interpersonal deception theory suggests that users process both verbal and non-verbal cues to make decisions about the credibility of the communicator (Burgoon & Buller, 1996). In the case of a cyber-attack, the stimulus is usually the deceptive information embedded in the attack. Users often engage and seek for such stimuli as they may contain information of value or interest.

Similarly, the theory of deception posits that most users follow a cognitive link or path that enables them to make judgements about the credibility of a stimulus that they are exposed to (Johnson, Grazioli, Jamal, & Zualkernan, 1992). Users base these judgements on similarities to either previous experience, or their inherent or trained technical ability. For example, some users interpret assurance mechanisms such as certificates, seals or testimonials as cues for

credibility based on their previous experiences (Chang, Cheung, & Tang, 2013; S. Grazioli & Jarvenpaa, 2000; Kim & Benbasat, 2006).Others process or interpret structural attributes of the stimulus and the information embedded within based on their inherent or acquired expertise (Jakobsson, Tsow, Shah, Blevis, & Lim, 2007; Vishwanath, Herath, Chen, Wang, & Rao, 2011). Research on phishing has shown cues such as source of the email, grammar, spelling and title as salient factors in detecting phishing attacks (Vishwanath et al., 2011).

Other studies suggest factors such as risk propensity, self-efficacy, personal knowledge and level of involvement are correlated with deception detection accuracy (Chen, Wang, Herath, & Rao, 2011; Vishwanath et al., 2011). Individual factors hypothesized to affect phishing detection accuracy include gender (Dhamija, Tygar, & Hearst, 2006), and personality traits such as commitment, trust and fear (Workman, 2008a). Underlying these factors is the idea that people process information to detect deception.

However, how people process information depends partly on their frame of mind. For example, it is widely recognized that users who are put into a cautious frame are less likely to be victimized by security attacks than those who are not (Biros et al., 2002; George, Marett, & Tilley, 2004). While this is recognized, most research does not take frame of mind into account when examining the empirical evidence.

2.1 Frame of Mind

There is plenty of research demonstrating that users' frames of mind impact their performance. As a simple illustration, the level of stress the user feels impacts performance (Mann, 2010). Furthermore, the activity a user performs directly impacts their frame of mind. For example, people on a mobile phone are distracted, and drivers who are in a distracted frame are four times more likely to have an accident (Redelmeier & Tibshirani, 1997).

This research attempts to test if the user's frame of mind impacts their deception detection ability. There are, of course, multiple ways to alter a user's frame of mind. In this research, we manipulate users' (1) need for information and (2) security consciousness.

2.1.1 Need for information

Most studies on security-related deception employ the context of email use and phishing (Jakobsson et al., 2007; Vishwanath et al., 2011; J. Wang, Chen, Herath, & Rao, 2009; Workman, 2008b). However, the majority of users spend time on the Internet on application types other than email. The question thus arises as to whether users engaged with web applications other than email are in a frame of mind different from users using email and hence are more or less vulnerable to security attacks. For example, a user's frame of mind when using a search engine is entirely different from that when he/she checks email or browses the web. It has been shown that users' need for information has an effect on their information processing and use patterns (Byström & Järvelin, 1995; Case, 2012). Thus, willingness to trust and use information will vary based on users' frames of mind when they seek information. However, there is little research that investigates this phenomenon. To understand how frame of mind impacts application use we turn to research on information seeking behaviour.

Information seeking behaviour is the purposive seeking of information to satisfy a specific goal (T. D. Wilson, 2000). The nature of this goal influences the user's frame of mind and defines relevant search behaviour, for example, whether to use automated information systems such as search engines or manual systems such as an online catalogue. Prior research argues there are three different types of frames in which the user is directly involved in

sourcing information – (1) Active seeking (2) Active scanning, and (3) Non-directed monitoring (Choo, Detlor, & Turnbull, 1998; McKenzie, 2003).

- **Active seeking** occurs when users look for information based on an already identified need or knowledge gap and perform a systematic search. The search process ends when the identified knowledge gap is filled. For example, a user employs a search engine to find a specific piece of information.
- **Active scanning** occurs when users' search processes are constrained to an already identified specific information-rich source. In active scanning, users do not have a specific goal or need in mind but are constantly aware of the possibility of finding useful new information. For example, users monitor their email or social networks regularly.
- **Non-directed monitoring** occurs when users serendipitously find information in an unlikely place; users do not have any goal in mind but their information need is triggered when they are exposed to useful information. On the Internet this would be the equivalent of finding an interesting article or video while browsing aimlessly from one website to another.

Consistent with the literature, we consider that users, subject to their information need, seek information by engaging in any of the three frames (Choo et al., 1998). However, each frame causes users to manifest a unique behaviour that in turn influences their processing abilities (Case, 2012).

2.1.2 Security consciousness

Another factor that affects users' frame of mind while using the Internet is the information already possessed by them. For example, research on framing effects demonstrates that depending upon how information is presented, users can be manipulated to make different decisions (Tversky & Kahneman, 1974). The literature points to three types of framing effects – (1) Attribute framing, (2) Risky choice framing and (3) Goal framing (Levin, Schneider, & Gaeth, 1998). In attribute framing, a single attribute of an object is the target of manipulation and is presented in an either positive or negative frame. When such a framing occurs, objects with a positive frame generally evaluate better than ones with a negative frame. In risky choice framing, usually only two options are presented to choose from – (a) a safe choice and (b) a risky gamble. Depending upon whether each choice is presented as a gain or a loss, users choose the safer or riskier option respectively (Tversky, Kahneman, & Choice, 1981). Finally, in goal framing users are usually encouraged to engage in some form of goal oriented activity. In doing so, information is presented in terms of the advantages of participating versus the disadvantages of not participating. In such cases, messages eliciting the negative consequences of not participating have been found to fare better in influencing participation (Levin et al., 1998).

The use of message framing to influence user behaviour is well documented in the literature. For example, in the marketing literature, the framing effects phenomenon is used to understand the effectiveness of product warning messages (e.g., on alcohol and cigarette packages) (Kelley, Gaidis, & Reingen, 1989; Strahan et al., 2002). In information systems, the effect of positive or negative frames has been explored to study IT adoption (Angst & Agarwal, 2009; Bhattacherjee & Sanford, 2006). In the context of information security, this has been demonstrated in testing the effects of warning on users' awareness of security issues (Biros et al., 2002; George et al., 2004; Stefano Grazioli, 2004). Accordingly, this study uses the concept of warning as a proxy for users' awareness or consciousness of security issues.

Whether or not users receive a warning about potential deception impacts their frame of mind by making them more suspicious. It has been established that when users' suspicion levels are aroused, they are better at detecting deception and that warnings are capable of arousing suspicion (Stiff, Kim, & Ramesh, 1992). However, not all studies of deception find a positive link between warning and deception detection performance (Stefano Grazioli & Wang, 2001; Marett & George, 2005). This discrepancy may be because most studies focus only on the presence or absence of a warning. Very few studies have explored the effect of the content of the warning. Accordingly, we draw ideas from the literature on framing effects and use both positively framed warning that highlights the consequential gains of adopting a particular behaviour, and negatively framed warning that highlights the consequential losses and test their effects on users' deception detection behaviour.

3. Proposed research model and Hypotheses

Based on the literature presented above, we present our research model as Figure 1 below. The two exogenous constructs are Information Seeking and Warning that together represent our 'frame of mind' concept. There are two endogenous constructs – (1) Attitude towards deception detection and (2) Deception detection behaviour. Attitude is defined as "a psychological tendency that is expressed by evaluating a particular entity with some degree of favour or disfavour" (Eagly & Chaiken, 1993). In this paper, we aim to measure users' general tendencies toward the threat of online deception. Users have a favourable attitude towards deception detection if they believe online deception exists and an unfavourable attitude if they believe no threat exists. Deception detection behaviour is the actual detection behaviour that users exhibit when exposed to online attacks. By comparing users' perceived attitude against their actual behaviour, we hope to generate unique insights about how online users make decisions in the face of deception. We present our arguments for our hypotheses below.

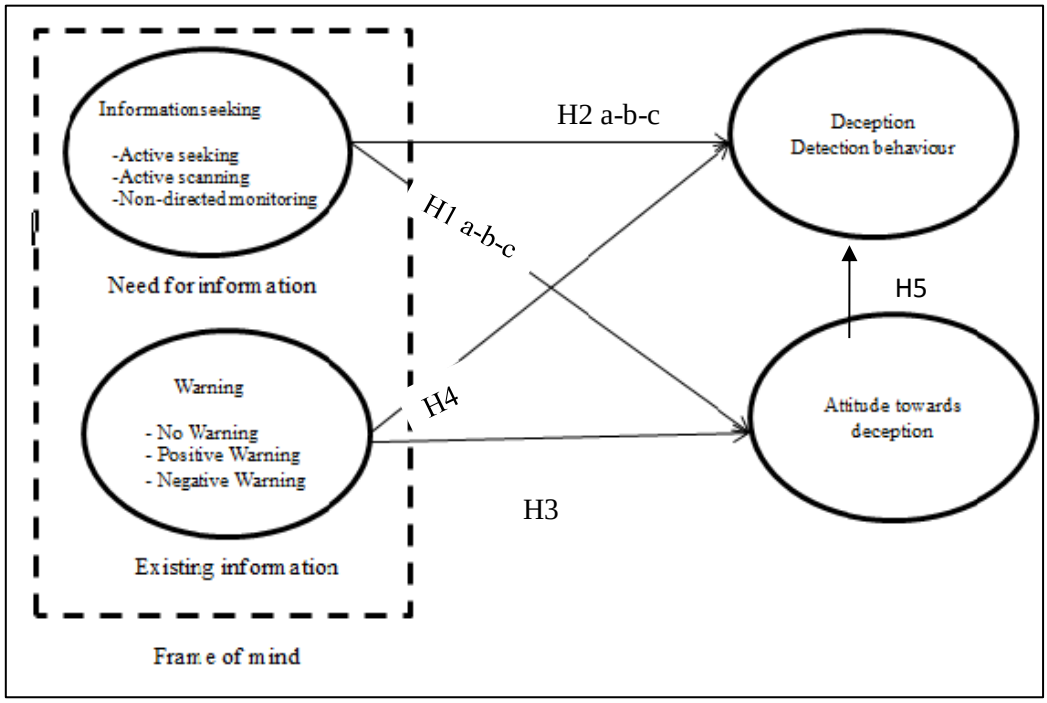

Figure 1: Research model

3.1 Effect of Information Seeking Frames

Active seeking. We argue that of the three information seeking frames – active scanning, active seeking and non-directed monitoring, users who actively seek information are the least likely to detect online attacks. Active seeking of information is a behaviour exhibited by individuals when they experience a gap in knowledge about a specific topic (T. D. Wilson, 1999). This leads them to carry out a systematic and pre-planned search effort to fill the knowledge gap. However, as the goal is knowledge acquisition, user behaviour is subject to the principle of least effort (Zipf, 1949); humans have a tendency to choose and use easily available information without considering the quality and reliability of the information (Bates, 2003). Methodologies that decrease the effort of information acquisition reduce reliance on the quality of information as a criterion (Hertzum, Andersen, Andersen, & Hansen, 2002; King, Casto, & Jones, 1994) .

Users engaged in the active seeking frame often use recommendation agents or search engines. Such systems reduce the effort of information acquisition and help users to easily make relevant decisions. However, the degree that such systems help the customer in decision making depends on the objective of the person who controls the system (Hill, King, & Cohen, 1996). A study of personal recommendation agents (PRA) demonstrated that deceptive PRAs can have a significant effect on product choice to users' detriment (Xiao, 2010). With the explosive growth of content on the web, it is increasingly becoming necessary to find information quickly and accurately. This makes users highly vulnerable to attacks such as search engine poisoning (Townsend, 2010). Accordingly, relative to the other two frames, we expect that users engaged in active seeking will be the most vulnerable to online attacks. Hence:

> *H1a: Of the three frames, Active seeking, Active scanning & Non-directed monitoring, users who are engaged in the Active Seeking frame will have the least favourable attitude towards detecting attacks.*

Similarly,

> *H2a: Of the three frames, Active seeking, Active scanning & Non-directed monitoring, users who are engaged in the Active Seeking frame will be the worst detectors of deception.*

Active scanning. When users perform active scanning, they often engage in ritualistic or habitual behaviour (Rubin, 1994) and place themselves in environments which are known to be information rich. Prior positive experiences drive users to revisit such information sources (McKenzie, 2003). Users of email and social networks are example cases of users engaged in active scanning.

When compared to active seeking and non-directed monitoring, we argue that users engaged in active scanning are the least vulnerable. Users in an active scanning frame of mind initially apply some effort in differentiating between different information rich sources before choosing a specific choice of source (Choo et al., 1998). Once they have chosen a source, for example, a specific social network or email, they build a mental profile of expected behaviours. Deviations from expected behaviour are treated with suspicion. Also, a lot of public awareness about attacks relevant to this frame, such as phishing and email spam, exists. Thus, users are generally more vigilant when consuming information in this frame of mind (Ivaturi & Janczewski, 2012). Accordingly, users engaged in active scanning are

relatively better at detecting deception than users in the other two frames of mind. Hence:

> *H1b: Of the three frames, Active seeking, Active scanning & Non-directed monitoring, users who are engaged in the Active Scanning frame will have the most favourable attitude towards detecting attacks.*

> *H2b: Of the three frames, Active seeking, Active scanning & Non-directed monitoring, users who are engaged in the Active Scanning frame will be the best detectors of deception.*

Non-directed monitoring. We argue that users engaged in a non-directed monitoring frame are more likely to detect deception than users in an active seeking frame but less likely than users in an active scanning frame of mind. Users in this frame are usually not aware of the need for information until they encounter it. This behaviour corresponds to Wilson's (1999) passive attention, Choo et al.'s (1998) undirected viewing and Ross's (1999) finding without seeking. Toms (2000) describes this process as serendipitous information seeking where users only recognize the usefulness of information when the information is encountered. Essentially, in this frame of mind, users have no a priori intent of finding information and so the behaviour is not driven by speed as it is for active seeking users.

Users in this frame usually scan large chunks of information from varied sources until something catches their attention. They do not scan the whole information horizon in a single movement but rather take a glimpse, look further at things that might interest them and then take another glimpse (Kwasnik, 1992). During this iterative process of 'discovery' and 'consumption', users tend not to have time to judge the quality or credibility of the content. They hence use heuristic shortcuts instead of carefully processing information which makes them more vulnerable to deception (Chaiken, 1980). Also, the sense of curiosity or joy of 'discovery' associated with this frame triggers a need for information that lowers users' level of care and attention, consequently leading to low levels of deception detection. Hence, users in this frame of mind are more vulnerable than active scanning users who are relatively less accustomed to this sense of 'discovery'. Thus:

> *H1c: Users who are in the Non-directed monitoring frame of mind will have a more favourable attitude towards detecting attacks than users engaged in Active seeking when compared to users in the Active scanning frame of mind.*

> *H2c: Users who are engaged in the Non-directed monitoring frame of mind will be better detectors of deception than users engaged in Active seeking when compared to users in the Active scanning frame of mind.*

3.2 Effect of Warning and Warning Frames

Extant research has shown that training and warning are broadly the two major counter attack mechanisms through which users can enhance their deception detection performance. Training is a formal way of building relevant and necessary security skills and competencies and hence it contributes to better performance in identifying anomalies (M. Wilson, Stine, & Bowen, 2009). However, it is not feasible to provide such training to everyone using the web. Warnings, on the other hand, contribute to better deception detection performance by inducing suspicion about the credibility of information.

Prior research reveals that individuals perform better at deception detection when their suspicion is aroused (Biros et al., 2002; Stiff et al., 1992). Explicit warnings about potential deception have the ability to raise suspicion. Hence, people who are given a warning are much better prepared than people who are not given a warning.

However, prior (non-security) research has shown that the way the message is framed has an effect on users' decision making abilities. Accordingly, it is useful to think about the content or framing of the warning which can in turn impact detection accuracy. Research on framing effects tells us that for behaviours that involve some level of risk or unpleasant outcomes, negatively framed messages that emphasize losses fare better than positively framed messages that focus on the gains (Rothman, Bartels, Wlaschin, & Salovey, 2006). As being victimized by an online attack can be considered as a high risk outcome and in line with the above argument, we propose that:

> *H3: Users who are given a negatively framed warning will have the most, users who are given no warning will have the worst and users who are given a positively framed warning will have a moderately favourable attitude towards deception.*

> *H4: Users who are given a negatively framed warning will have the best, users who are given no warning will have the worst and users who are given a positively framed warning will have moderate deception detection behaviour.*

3.3 Deception Detection Behaviour

Finally, we explore whether users' attitude towards detecting attacks has an influence on their actual deception detection behaviour. The positive influence of users' attitude on users' eventual behaviour via users' intentions is well established in the literature (Ajzen, 1991; Ajzen & Fishbein, 1977). This relationship has also been tested in the context of adoption and use of IT in different contexts and across cultures (Davis, 1989; Venkatesh, Morris, Davis, & Davis, 2003). Accordingly,

> *H5: Users' attitude towards deception detection is positively related to their actual deception detection behaviour*

4. Methodology

Hypotheses will be tested through a quasi-experiment conducted in a laboratory setting (Cook, Campbell, & Day, 1979). The experiment will use a repeated measures design that expose subjects to three simulated online attacks relevant to the three information seeking frames. The quasi-experiment will comprise of an experimental task phase and a post-experimental phase.

Sample. Subjects will be undergraduate students of a large business school. The literature supports the use of business students as a representative sample for experimental studies in IS, especially when the target population is that of typical Internet users (Dickson, Senn, & Chervany, 1977; Gefen, Karahanna, & Straub, 2003). Also, benchmark studies such as the Pew Internet project indicate that users who spend the most time on the Internet are in the same age bracket as university students (Pew, 2012). Subjects will be recruited through an advertisement. There will be a monetary incentive to motivate potential subjects to take part in the experiment. We expect to recruit around 100 students and as we are using a repeated measures design our effective sample size will be 300 (with three tasks assigned per subject).

4.1 Experimental Procedure

4.1.1 Pre-experimental phase

In this phase, subjects will be asked to complete a survey that collects information about users' age groups and gender. Also, subjects will be briefed about the nature of the task and time frame involved in participating in the experiment.

4.1.2 Experimental task phase

During this phase, subjects will be directed to a website where they will be given three treatments in a random order. The process for each treatment will be similar. Subjects will first be given a set of instructions to complete each treatment task. Each treatment will simulate the "typical" experience of a user engaged in each of the three information seeking frames discussed earlier.

For the active seeking treatment, subjects will be asked to find answers to hypothetical questions using a custom search engine. This task replicates user behaviour while engaged in an active seeking frame. The search results will be manipulated to mimic a search engine poisoning attack – the most prominent attack method to affect users of search engines (Howard & Komili, 2010; John, Yu, Xie, Krishnamurthy, & Abadi, 2011). Specifically, the search engine would query Microsoft Bing, and return Bing results. However, a random 30% of the results will be replaced by dummy URLs irrelevant to users' original queries. The manipulations will include a mismatch between the displayed URL and the destination URL and changes to the description of the search result snippet. These manipulations are in line with standard search engine poisoning attacks. A ratio of the number of clicks on manipulated results over the total number of clicks was taken as an aggregate measure of users' deception detection behaviour.

For the active scanning treatment, subjects will be asked to login to an email account created for the study. Subjects will be told to treat the email inbox as their own and take any appropriate action. Each subject will receive a unique email account to make it easier for the researchers to track individual behaviour. Some of the emails in this treatment will be crafted as phishing emails. Again, the ratio of the number of clicks on manipulated links in the phishing emails over the total number of clicks on links across all the emails will be taken as the aggregate measure.

For non-directed monitoring, subjects will be asked to browse a news portal that will provide three categories of news articles – business, sports and entertainment. The instructions will be to spend time browsing the three categories and to identify one article per category that users find most useful and interesting. This task replicates the exploratory nature of non-directed monitoring. All user clicks on the news portal will be recorded and a ratio of the number of clicks on manipulated links over the total number of clicks will be calculated to represent individual subjects' deception detection rate.

All subjects will be kept ignorant of the real nature of the study. $1/3^{rd}$ of subjects will be treated with a negatively framed warning, and $1/3^{rd}$ with a positively framed warning. The rest will not receive any warning.

4.1.3 Post-experimental phase

Once the three tasks are completed, subjects will be directed to the post-experimental survey that measures users' attitude towards deception. The items used for the study will be adapted from the literature as a 7-point semantic differential scale with polar adjectives (Jingguo

Wang, Chaudhury, & Rao, 2008). Example polar adjectives used are extremely foolish-extremely wise and extremely risky-extremely safe.

5. Analysis

In order to understand the effect of different contexts of information seeking and warning frames, tests for group differences will be carried out. ANOVA tests are simple yet powerful and are used to test the effect of a manipulation variable on the dependent variable in an experimental study. In fact, as there are multiple dependent variables (attitude and deception behaviour) we will use a MANOVA in order to test for the group differences.

6. Conclusion and Expected contributions

This study is meant to provide several contributions to both academics and practitioners. From the theoretical perspective, this research makes important contributions to the user deception detection literature. As far as we know, this is the first study in IS security domain that considers the heterogeneous nature of user vulnerability by testing the effect of various user contexts of information seeking as a predictor for user vulnerabilities. From a practitioner's perspective, this study offers empirical evidence that trainings and awareness programmes should go beyond the traditional anti-phishing trainings to include information about emerging attacks such as search engine poisoning.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin; Psychological Bulletin, 84*(5), 888.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339-370.

Bates, M. (2003). Toward An Integrated Model of Information Seeking and Searching. *Graduate School of Education and Information Studies*. doi:citeulike-article-id:1413170

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly*, 805-825.

Biros, D. P., George, J. F., & Zmud, R. W. (2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly*, 119-144.

Burgoon, J. K., & Buller, D. B. (1996). Interpersonal Deception Theory. *Communication Theory, 6*(3), 311-328. doi:10.1111/j.1468-2885.1996.tb00132.x

Byström, K., & Järvelin, K. (1995). Task complexity affects information seeking and use. *Information Processing & Management, 31*(2), 191-213.

Case, D. O. (2012). *Looking for information: A survey of research on information seeking, needs, and behavior*: Emerald Group Publishing.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology, 39*(5), 752.

Chang, M. K., Cheung, W., & Tang, M. (2013). Building Trust Online: Interactions among Trust Building Mechanisms. *Information & Management*.

Chen, R., Wang, J., Herath, T., & Rao, H. R. (2011). An investigation of email processing from a risky decision making perspective. *Decision Support Systems, 52*(1), 73-81. doi:10.1016/j.dss.2011.05.005

Choo, C. W., Detlor, B., & Turnbull, D. (1998). *A Behavioral Model of Information Seeking on the Web - Preliminary Results of a Study of How Managers and IT Specialists Use the Web.* Paper presented at the Proceedings of the 61st Annual Meeting of the American Society of Information Science, Pittsburgh, PA.

Cook, T. D., Campbell, D. T., & Day, A. (1979). *Quasi-experimentation: Design & analysis issues for field settings*: Houghton Mifflin Boston.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works.* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Dickson, G. W., Senn, J. A., & Chervany, N. L. (1977). Research in management information systems: The Minnesota experiments. *Management Science, 23*(9), 913-934.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*: Harcourt Brace Jovanovich College Publishers.

Ekman, P. (2009). *Telling lies: Clues to deceit in the marketplace, politics, and marriage*: WW Norton & Company.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 51-90.

George, J. F., Marett, K., & Tilley, P. (2004). *Deception detection under varying electronic media and warning conditions.* Paper presented at the System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on.

Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. *Group Decision and Negotiation, 13*(2), 149-172. doi:10.1023/B:GRUP.0000021839.04093.5d

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 30*(4), 395-410.

Grazioli, S., & Wang, A. (2001). *Looking Without Seeing: Understanding Unsophisticated Consumers' Success and Failure to Detect Internet Deception.* Paper presented at the ICIS 2001 Proceedings.

Hertzum, M., Andersen, H. H. K., Andersen, V., & Hansen, C. B. (2002). Trust in information sources: seeking information from people, documents, and virtual agents. *Interacting with Computers, 14*(5), 575-599. doi:10.1016/s0953-5438(02)00023-1

Hill, D. J., King, M. F., & Cohen, E. (1996). The perceived utility of information presented via electronic decision aids: A consumer perspective. *Journal of Consumer Policy, 19*(2), 137-166. doi:10.1007/bf00412471

Howard, F., & Komili, O. (2010). Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware. *Sophos Technical Papers*.

Ivaturi, K., & Janczewski, L. (2012). *A typology of social engineering attacks – an information science perspective.* Paper presented at the PACIS 2012 Proceedings. Paper 219, Ho Chi Minh city, Vietnam.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y.-K. (2007. *What instills trust? a qualitative study of phishing*. Paper presented at the Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security, Scarborough, Trinidad and Tobago.

John, J. P., Yu, F., Xie, Y., Krishnamurthy, A., & Abadi, M. (2011). *deSEO: Combating search-result poisoning.* Paper presented at the Proceedings of the 20th USENIX conference on Security.
Johnson, P. E., Grazioli, S., Jamal, K., & Glen Berryman, R. (2001). Detecting deception: adversarial problem solving in a low base-rate world. *Cognitive Science, 25*(3), 355-392. doi:10.1016/s0364-0213(01)00040-4
Johnson, P. E., Grazioli, S., Jamal, K., & Zualkernan, I. A. (1992). Success and failure in expert reasoning. *Organizational Behavior and Human Decision Processes, 53*(2), 173-203. doi:10.1016/0749-5978(92)90061-b
Kelley, C. A., Gaidis, W. C., & Reingen, P. H. (1989). The use of vivid stimuli to enhance comprehension of the content of product warning messages. *Journal of Consumer Affairs, 23*(2), 243-266.
Kim, D., & Benbasat, I. (2006). The effects of trust-assuring arguments on consumer trust in internet stores: Application of Toulmin's model of argumentation. *Information Systems Research, 17*(3), 286-300.
King, D. W., Casto, J., & Jones, H. (1994). *Communication by engineers : a literature review of engineers' information needs, seeking processes, and use.* Council on Library Resources, Washington D.C.
Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*: Springer.
Kwasnik, B. H. (1992. *A Descriptive Study of the Functional Components of Browsing*. Paper presented at the Proceedings of the IFIP TC2/WG2.7 Working Conference on Engineering for Human-Computer Interaction.
Levin, I. P., Schneider, S. L., & Gaeth, G. J. (1998). All frames are not created equal: A typology and critical analysis of framing effects. *Organizational Behavior and Human Decision Processes, 76*(2), 149-188.
Mann, I. (2010). *Hacking the human: social engineering techniques and security countermeasures*: Gower Publishing, Ltd.
Marett, K., & George, J. F. (2005, 03-06 Jan. 2005). *Group Deception in Computer-Supported Environments.* Paper presented at the System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on.
McKenzie, P. (2003). A model of information practices in accounts of everyday-life information seeking. *Journal of Documentation, 59*(1).
Menn, J. (2010). *Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet*: PublicAffairs Store.
Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element of Security.
Norton. (2010). Norton's Cybercrime Report: The Human Impact. from http://community.norton.com/t5/Ask-Marian/Norton-s-Cybercrime-Report-The-Human-Impact-Reveals-Global/ba-p/282432
Pew. (2012). Demographics of Internet Users. Retrieved 1/04/2013, from http://pewinternet.org/Trend-Data-(Adults)/Whos-Online.aspx
Redelmeier, D. A., & Tibshirani, R. J. (1997). Association between cellular-telephone calls and motor vehicle collisions. *New England Journal of Medicine, 336*(7), 453-458.
Ross, S. C. (1999). Finding without seeking: the information encounter in the context of reading for pleasure. *Information Processing & Management, 35*(6), 783-799. doi:10.1016/s0306-4573(99)00026-6
Rothman, A. J., Bartels, R. D., Wlaschin, J., & Salovey, P. (2006). The Strategic Use of Gain-and Loss-Framed Messages to Promote Healthy Behavior: How Theory Can Inform Practice. *Journal of Communication, 56*(s1), S202-S220.

Rubin, A. M. (1994). Media uses and effects: A uses-and-gratifications perspective. In J. B. D. Zillmann (Ed.), *Media effects: Advances in theory and research* (pp. 417-436). Hillsdale, NJ, England: Lawrence Erlbaum Associates, Inc.

Stiff, J. B., Kim, H. J., & Ramesh, C. N. (1992). Truth biases and aroused suspicion in relational deception. *Communication Research, 19*(3), 326-345.

Strahan, E. J., White, K., Fong, G. T., Fabrigar, L. R., Zanna, M. P., & Cameron, R. (2002). Enhancing the effectiveness of tobacco package warning labels: a social psychological perspective. *Tobacco control, 11*(3), 183-190.

Toms, E. G. (2000). *Serendipitous Information Retrieval.* Paper presented at the In Proceedings of DELOS Workshop: Information Seeking, Searching and Querying in Digital Libraries.

Townsend, K. (2010). The art of social engineering. *Infosecurity, 7*(4), 32-35.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science, 185*(4157), 1124-1131. doi:10.1126/science.185.4157.1124

Tversky, A., Kahneman, D., & Choice, R. (1981). The framing of decisions. *Science, 211*, 453-458.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. doi:10.1016/j.dss.2011.03.002

Wang, J., Chaudhury, A., & Rao, H. R. (2008). Research Note—A Value-at-Risk Approach to Information Security Investment. *Information Systems Research, 19*(1), 106-120. doi:doi:10.1287/isre.1070.0143

Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). An exploration of the design features of phishing attacks. *Information Assurance, Security and Privacy Services, 4*, 259.

Wilson, M., Stine, K., & Bowen, P. (2009). Information Security Training Requirements: A Role- and Performance-Based Model *NIST Special Publication 800-16*.

Wilson, T. D. (1999). Models in information behaviour research. *Journal of Documentation, 55*(3), 249-270.

Wilson, T. D. (2000). Human information behavior. *Informing science, 3*(2), 49-56.

Workman, M. (2008a). A test of interventions for security threats from social engineering. *Information Management & Computer Security, 16*(5), 463-483.

Workman, M. (2008b). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674. doi:10.1002/asi.20779

Xiao, B. (2010). *Product-related deceptive information practices in B2C E-commerce: Formation, Outcomes, and Detection.* (The University of British Columbia Vancouver).

Zipf, G. K. (1949). *Human behavior and the principle of least effort*. Oxford, England: Addison-Wesley Press.